authorized user. If so, the access server **106** generates or retrieves the key (e.g., key A) that corresponds to that credential or otherwise enables access to a requested service. The access server may then, for example, send the key to the access device **102** (block **218**). Typically, the cryptographic processor **124** will encrypt the key to protect it during transmission. Here, the cryptographic processor may use a negotiated key or the public key associated with the private key to encrypt key A.

[**0064**] Once the access device **102** receives encrypted key A, the cryptographic processor decrypts key A and uses it to, for example, establish a connection with a network (block **220**).

[**0065**] Referring now to **FIG. 3** additional details of the authentication process will be discussed. **FIG. 3** illustrates one embodiment of a system **300** constructed in accordance with the invention where one or more users (not shown) may use one or more access devices **302** and **304** to access services **330** (e.g., connect to a data network) via an access server **306**. For example, to access a service a user presents authentication information (e.g., credentials **308** such as a password) to the access device **302** via a proximate input device (not shown). For convenience the term "credential(s)" may be used to refer generally to any type of information that a user may present for authentication purposes.

[**0066**] The access device **302** may include a security module that provides cryptographic processing and may incorporate other security mechanisms. For example, a security module may include one or more cryptographic processors **328** that perform cryptographic operations such as encryption, decryption, authentication, verification and signing. Using the security module, the access device **302** may authenticate the credentials received from the input device and securely send the credentials to a key manager **310** in the access server **306**.

[**0067**] The key manager **310** provides a secure environment for generating, assigning and maintaining keys that are used in the system. The key manager includes one or more cryptographic processors **324** for securely performing cryptographic operations including encryption, decryption, authentication, etc. The key manager also includes a secure data memory **322** for storing keys **326** in a manner that prevents the keys from being accessed by unauthorized persons or methods.

[**0068**] To provide secure processing and key storage a security boundary is associated with and enforced by the key manager. This security boundary may be established, for example, using hardware and/or cryptographic techniques.

[**0069**] Hardware techniques for providing a security boundary may include, for example, placing components within a single integrated circuit. In addition, one or more integrated circuits may be protected by a physical structure using tamper evident and/or tamper resistant techniques such as epoxy encapsulation.

[**0070**] Encryption techniques for establishing a security boundary may include, for example, encrypting any sensitive information before it leaves the key manager. For this purpose, the key manager may use one or more of the cryptographic processors **324** and store the associated encryption/decryption keys **326** in an internal secure data memory **322**.

[**0071**] To maintain the security of the system **300**, any keys distributed by the key manager to other components in the system should be adequately protected. For example, provisions may be made to ensure that keys are only delivered to authorized devices. In addition, provisions may be made to protect the keys during distribution and within the recipient devices.

[**0072**] In some embodiments the access device **302** includes one or more cryptographic processors **328** and keys (e.g., key **314**) to authenticate information that is sent from the access device **302** to the access server **306**, to facilitate secure transmission of keys to the access device **302**, and to protect the keys used by the access device **302**.

[**0073**] For example, using digital certificates and other cryptographic processes the access device **302** may provide strong authentication to the access server **306** that the credentials it sends to the access server **306** are from a user that is using that specific access device. In addition, these processes may be used to verify that the access device **302** provides a high level of protection for key material.

[**0074**] Once this authentication is provided to the access server **306**, the key manager **310** may safely distribute keys to the access device **302** to facilitate access to the desired service. For example, the key manager may distribute keys to the access device to enable the access device to connect to a data network.

[**0075**] The embodiment of **FIG. 3** provides an efficient mechanism that enables a user to, for example, use a variety of access devices to gain access to a network. Here, the user initially authenticates himself or herself to each device. The access server then automatically builds the network by distributing the necessary keys to each device. As described herein this process may be accomplished with a high level of security. Moreover, since the access server provides the appropriate keys to each device, the key material does not need to be given to the user. In addition, the user may not be required to, for example, provide a digital certificate to each access device he or she uses in the network.

[**0076**] Selected operations of the system **300** will be explained in more detail in conjunction with the flowchart of **FIG. 4**. As represented by block **402**, one or more keys may be generated to enable the access device to securely communicate with the access server. In some embodiments, this is accomplished through the use of asymmetric keys.

[**0077**] For example, a unique asymmetric identity key **314** may be provided for each access device. The private key portion of this asymmetric key may be stored within a security boundary (represented by dashed line **312**) in the access device. For example, a cryptographic processor **328** may generate the key within this security boundary and the private portion of the key may never be allowed to appear outside of the security boundary **312** in the clear (i.e., unencrypted). Additional details of a security boundary are provided below.

[**0078**] The public portion of the key may then be published with a digital certificate. For example, the manufacturer of the access device may publish the public key and the certificate on a publicly accessible server. The certificate serves to verify that the public key is authentic, that the private key has not been disclosed outside the security boundary and that the access device that holds the private